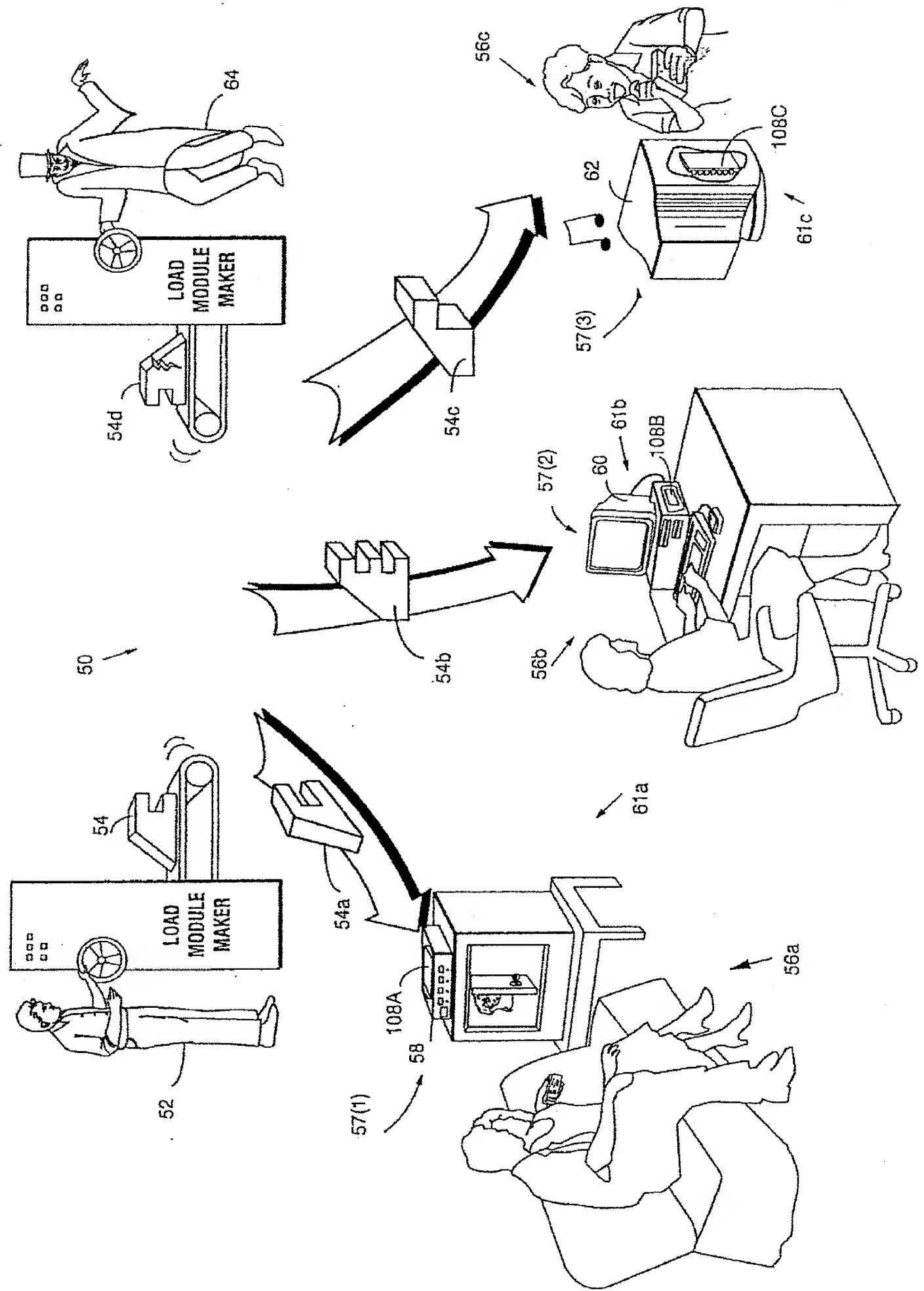
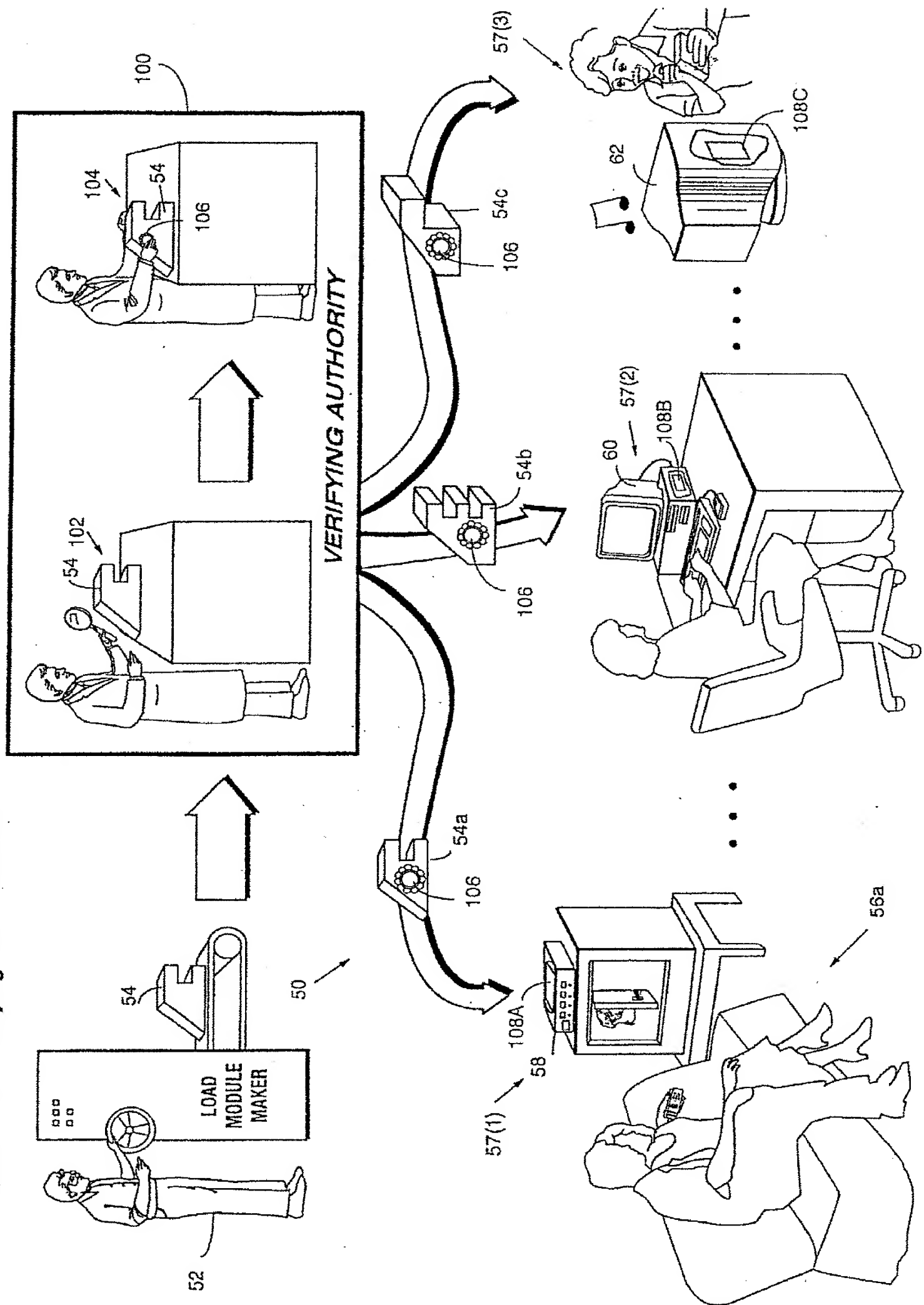


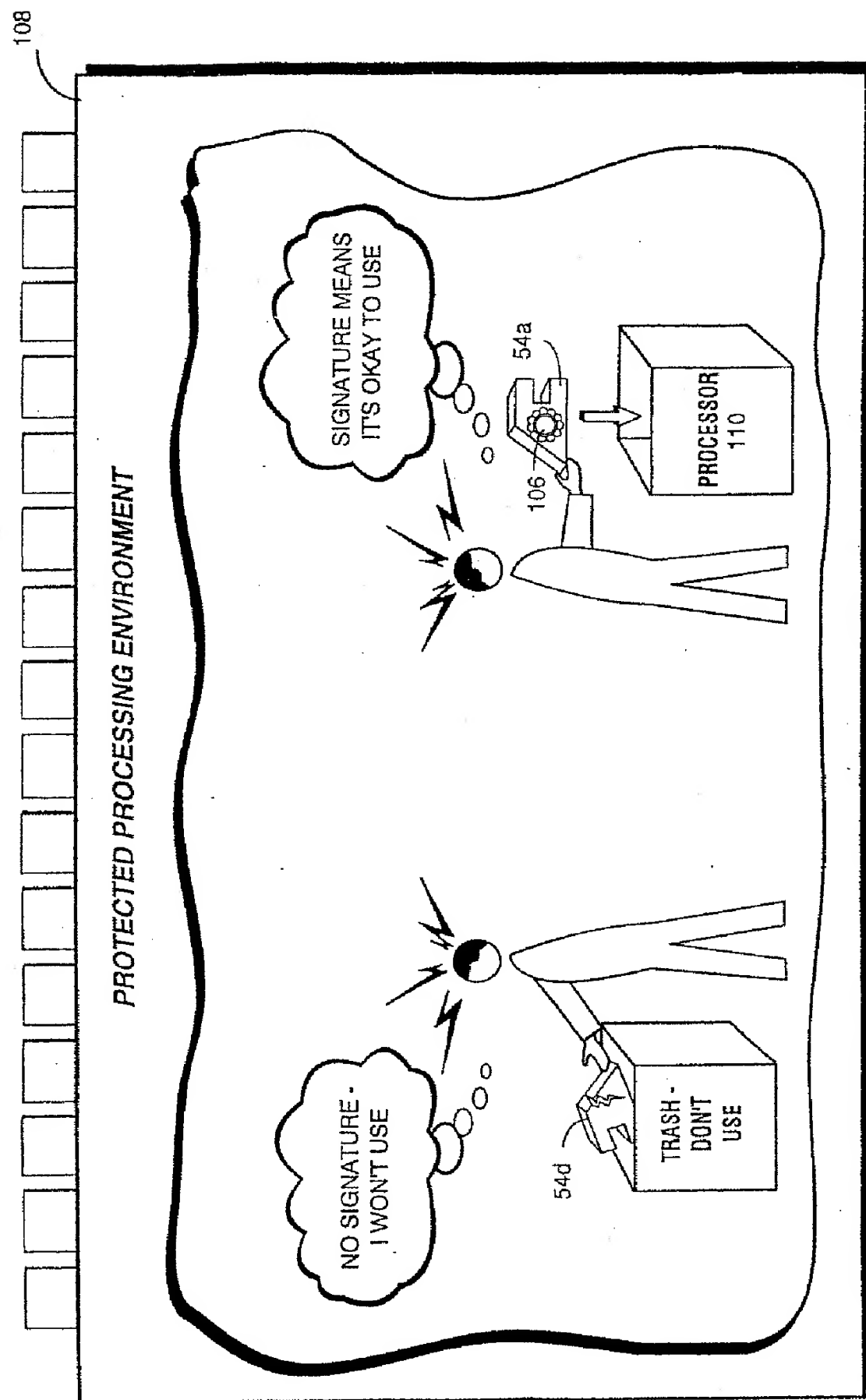
**FIG. 1** Defective or "Bogus" Load Modules Can Cause Problems



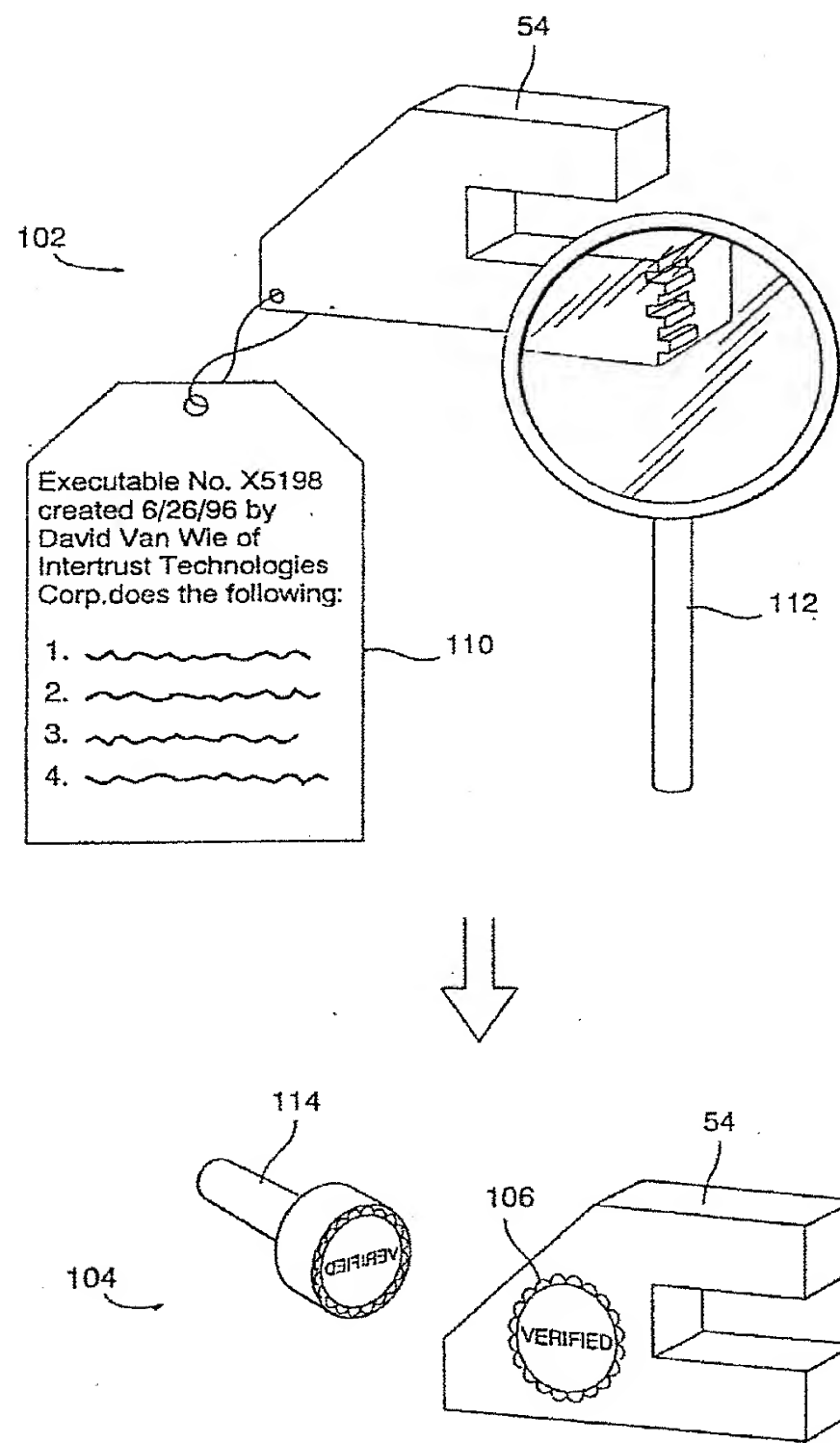
**FIG. 2** Verifying Load Modules



**FIG. 3** Before Protected Processing Environment Uses A Load Module, It Checks To See If Load Module Has Been Verified



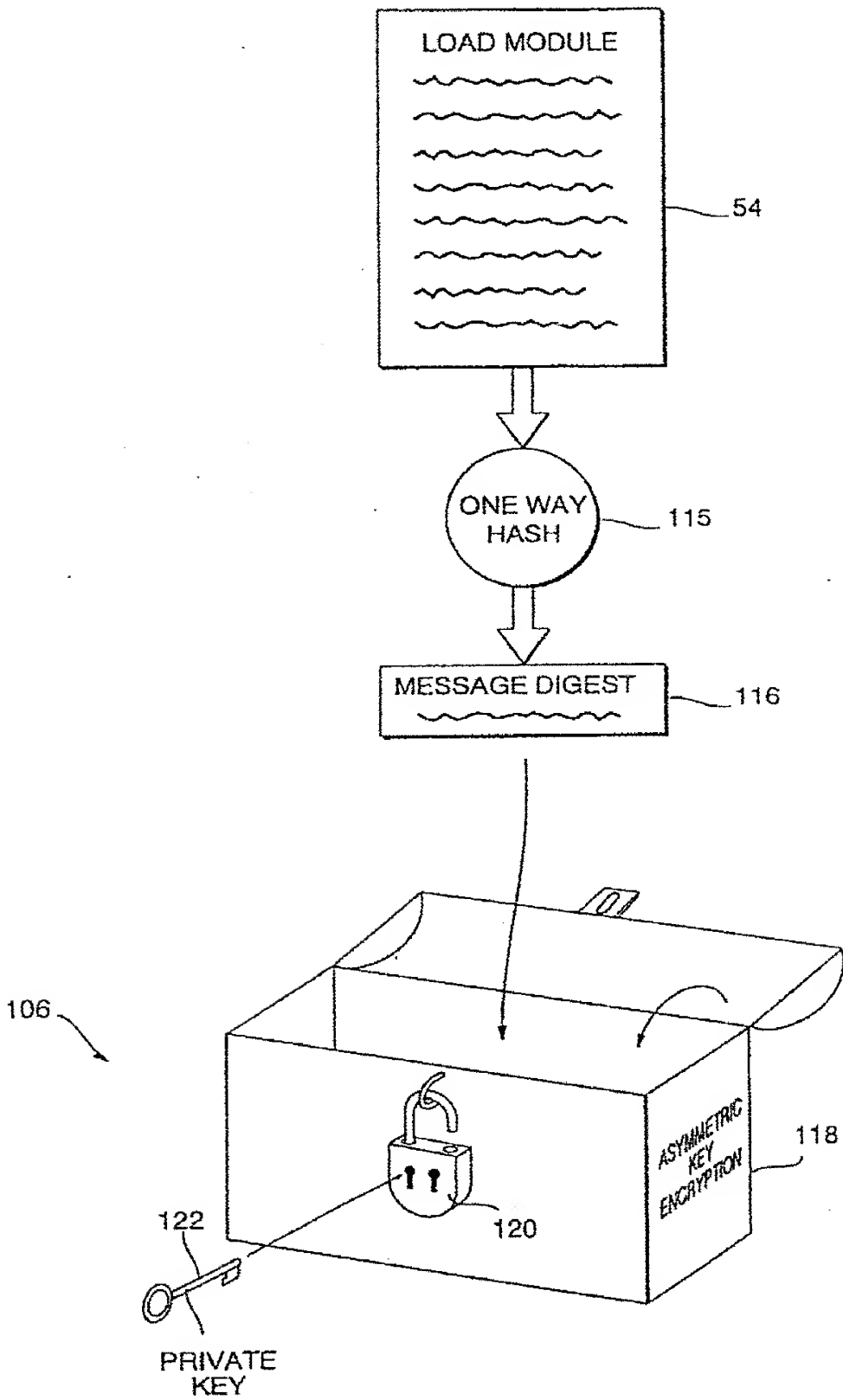
REPLACEMENT SHEET



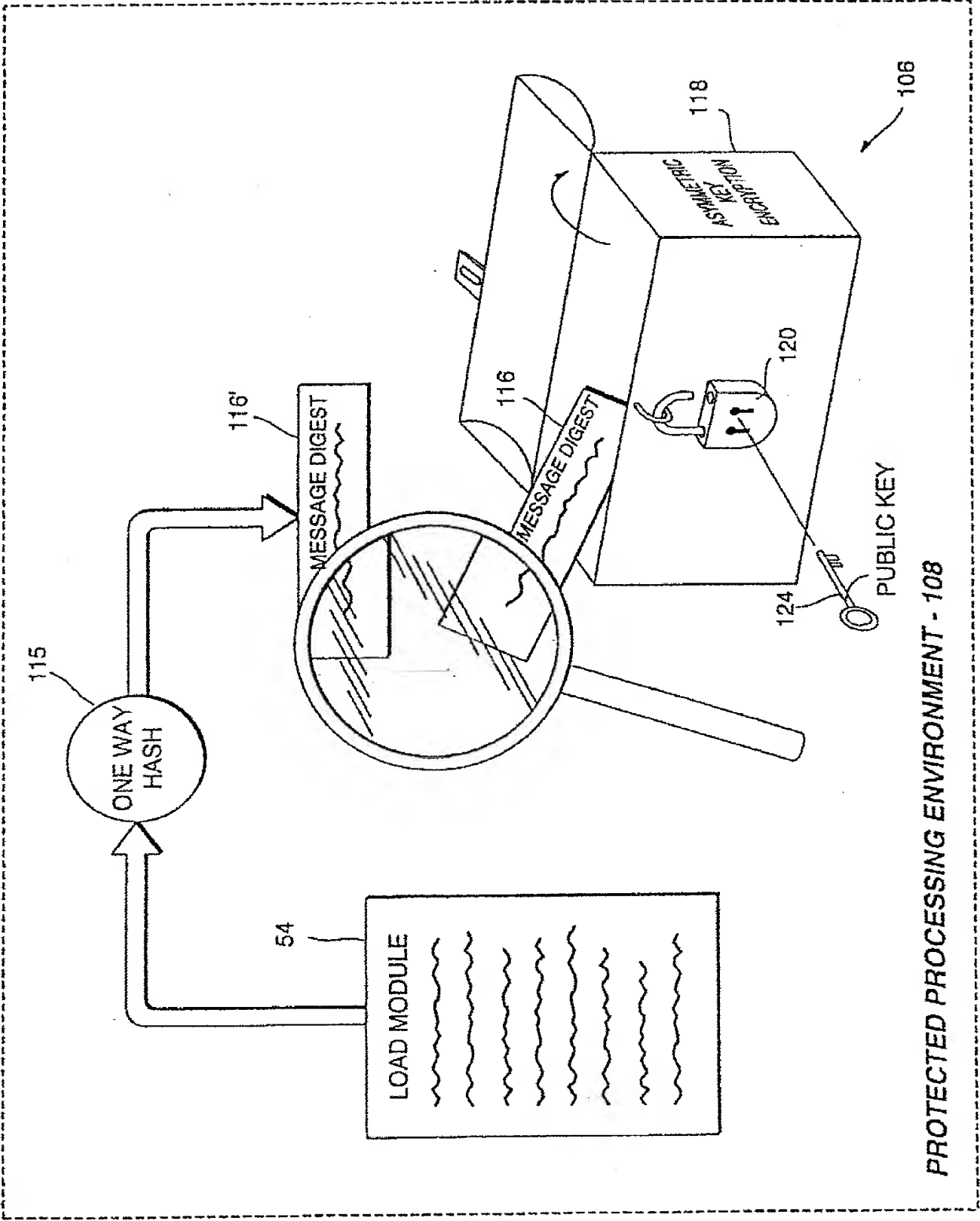
**FIG. 4**

**Certifying Load Module by  
Checking it Against its Documentation**

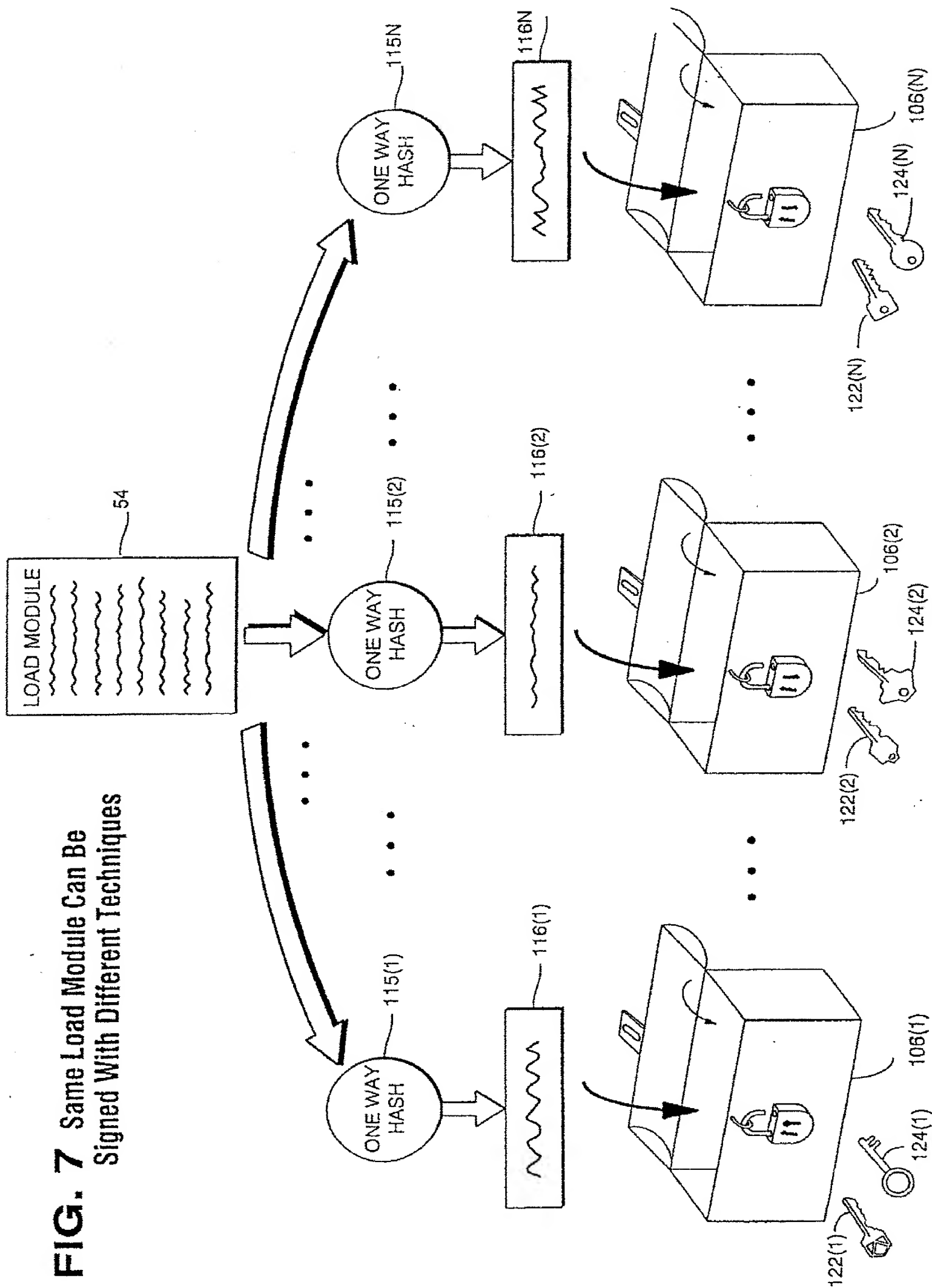
REPLACEMENT SHEET



**FIG. 5**  
Creating a Certifying  
Digital Signature



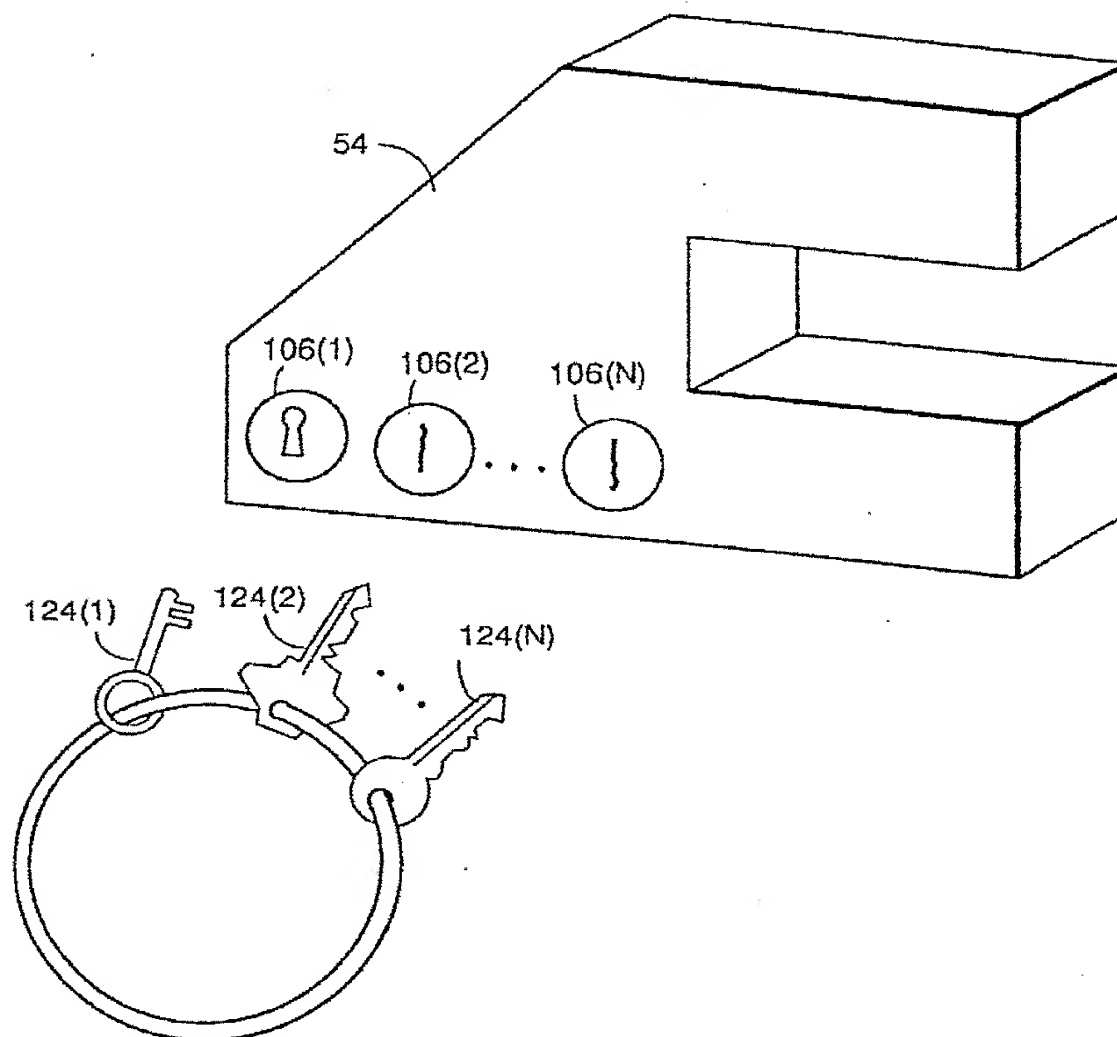
**FIG. 6** Authenticating a Digital Signature



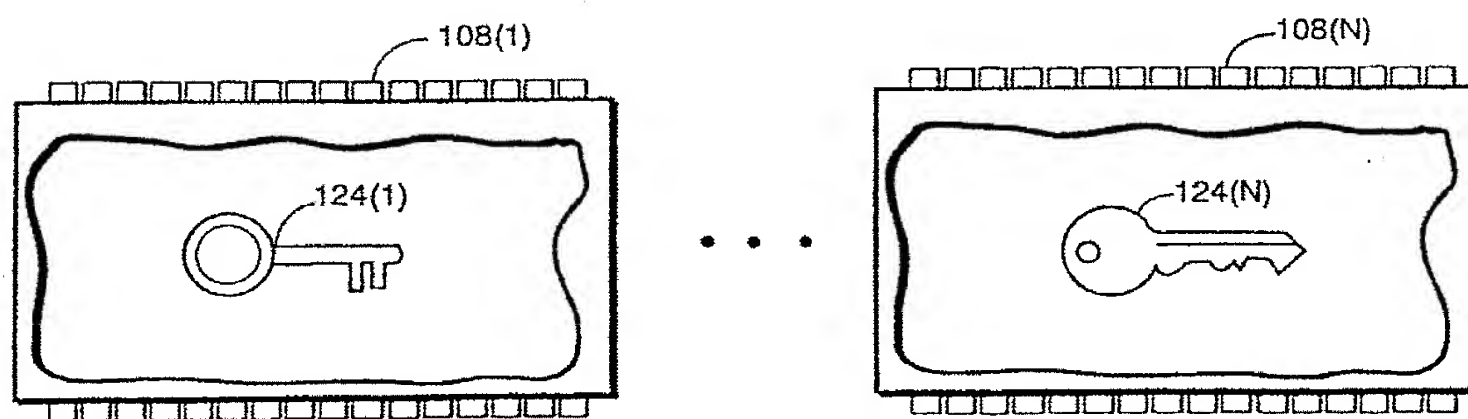
**FIG. 7** Same Load Module Can Be Signed With Different Techniques

# REPLACEMENT SHEET

**FIG. 8** Same Load Module Can Be Distributed with Multiple Signatures



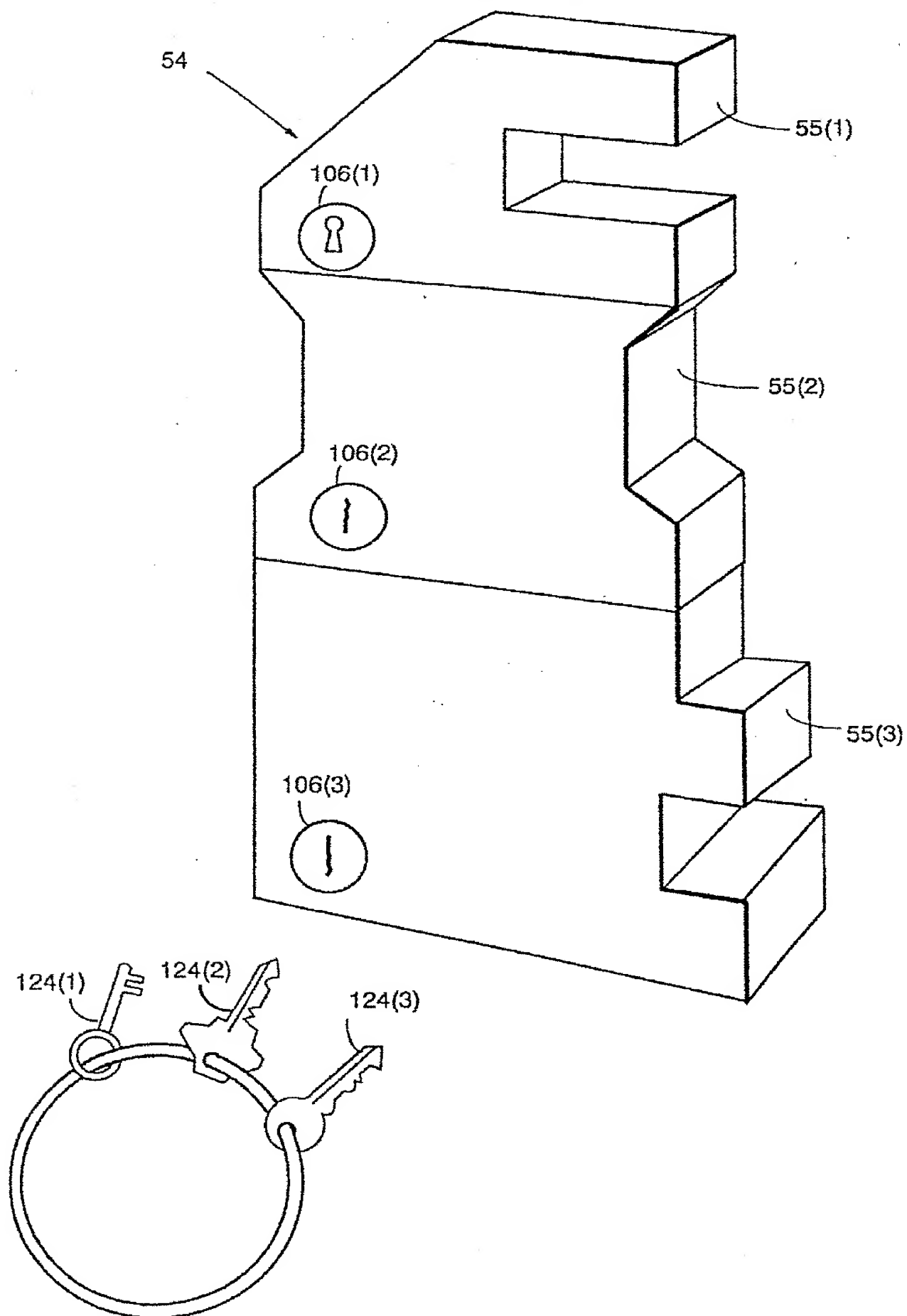
**FIG. 8A** Different Processing Environments Can Have Different Subsets of Keys



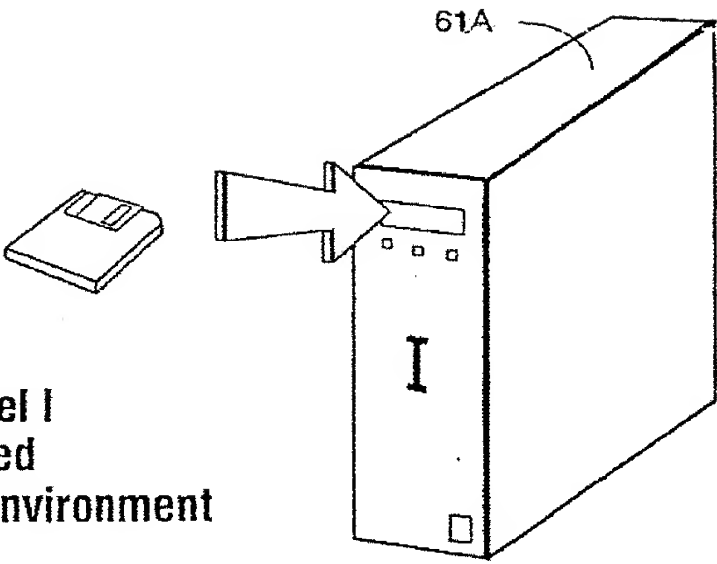


# REPLACEMENT SHEET

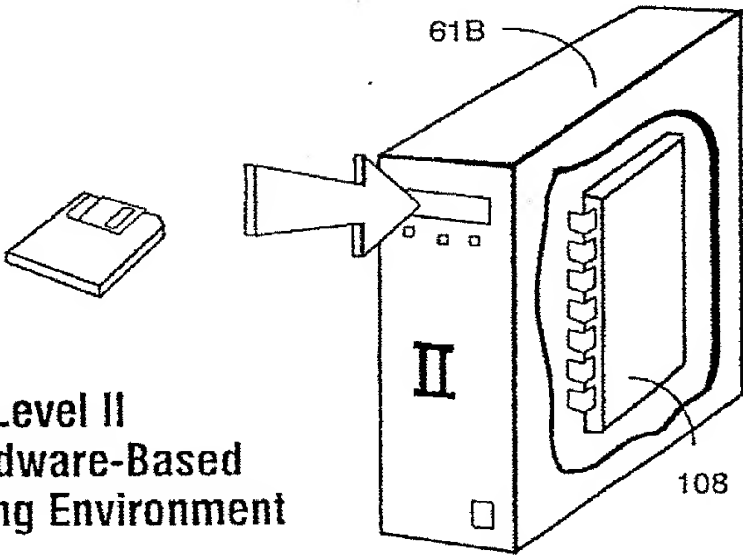
**FIG. 9** Load Module Can Have Several Independently Signed Portions



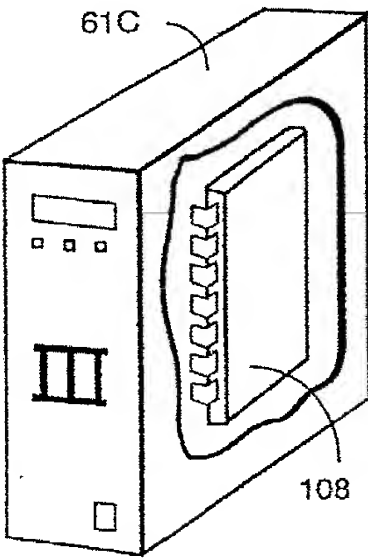
REPLACEMENT SHEET



**FIG. 10A** Assurance Level I  
Software-Based  
Protected Processing Environment



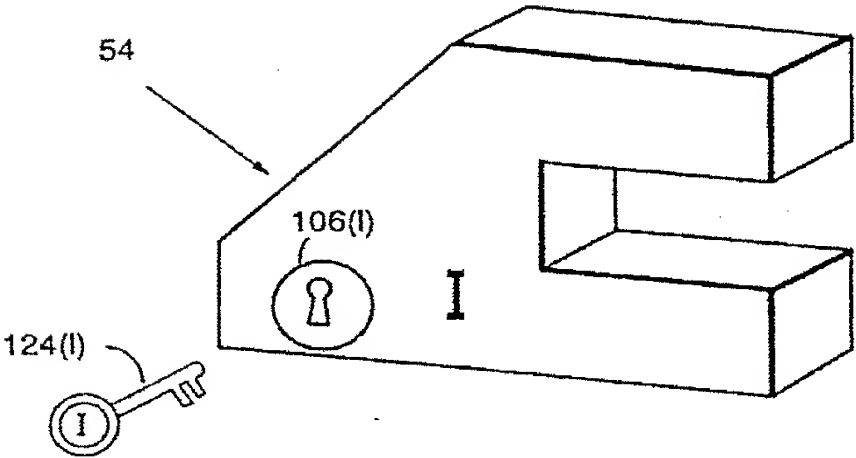
**FIG. 10B** Assurance Level II  
Software and Hardware-Based  
Protected Processing Environment



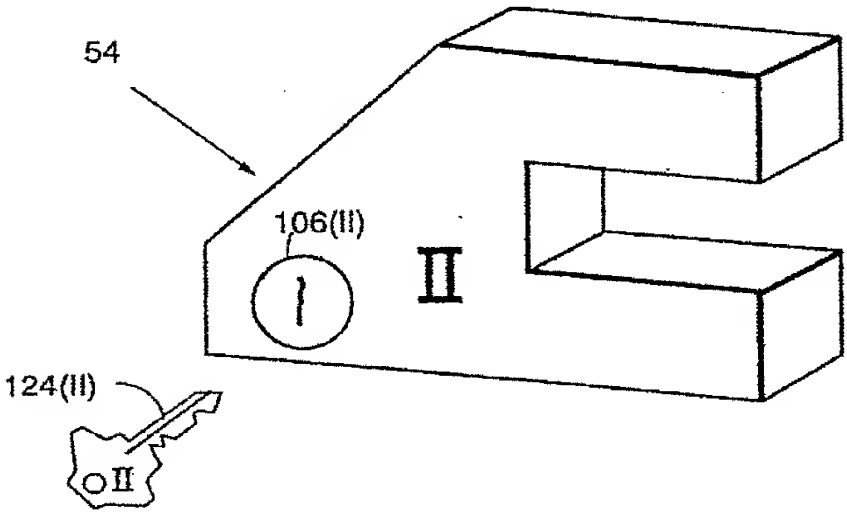
**FIG. 10C** Assurance Level III  
Hardware-Based  
Protected Processing Environment

REPLACEMENT SHEET

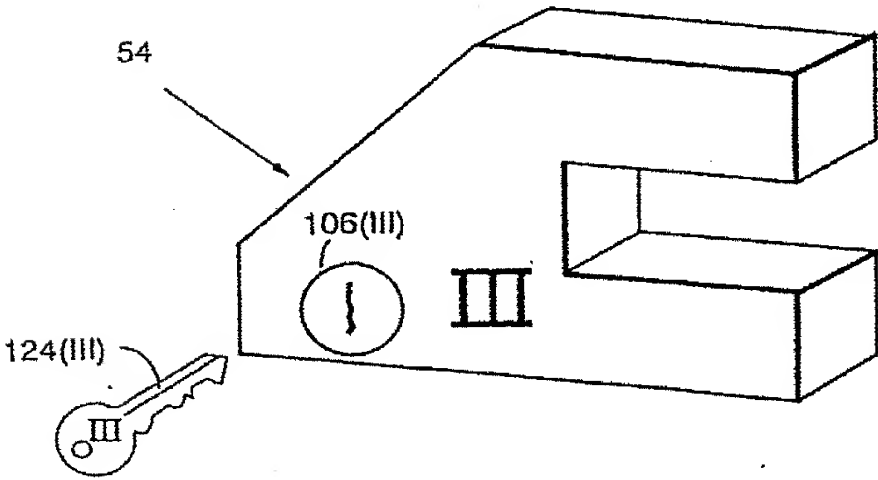
**FIG. 11A** Level I  
Digital Signature



**FIG. 11B** Level II  
Digital Signature



**FIG. 11C** Level III  
Digital Signature



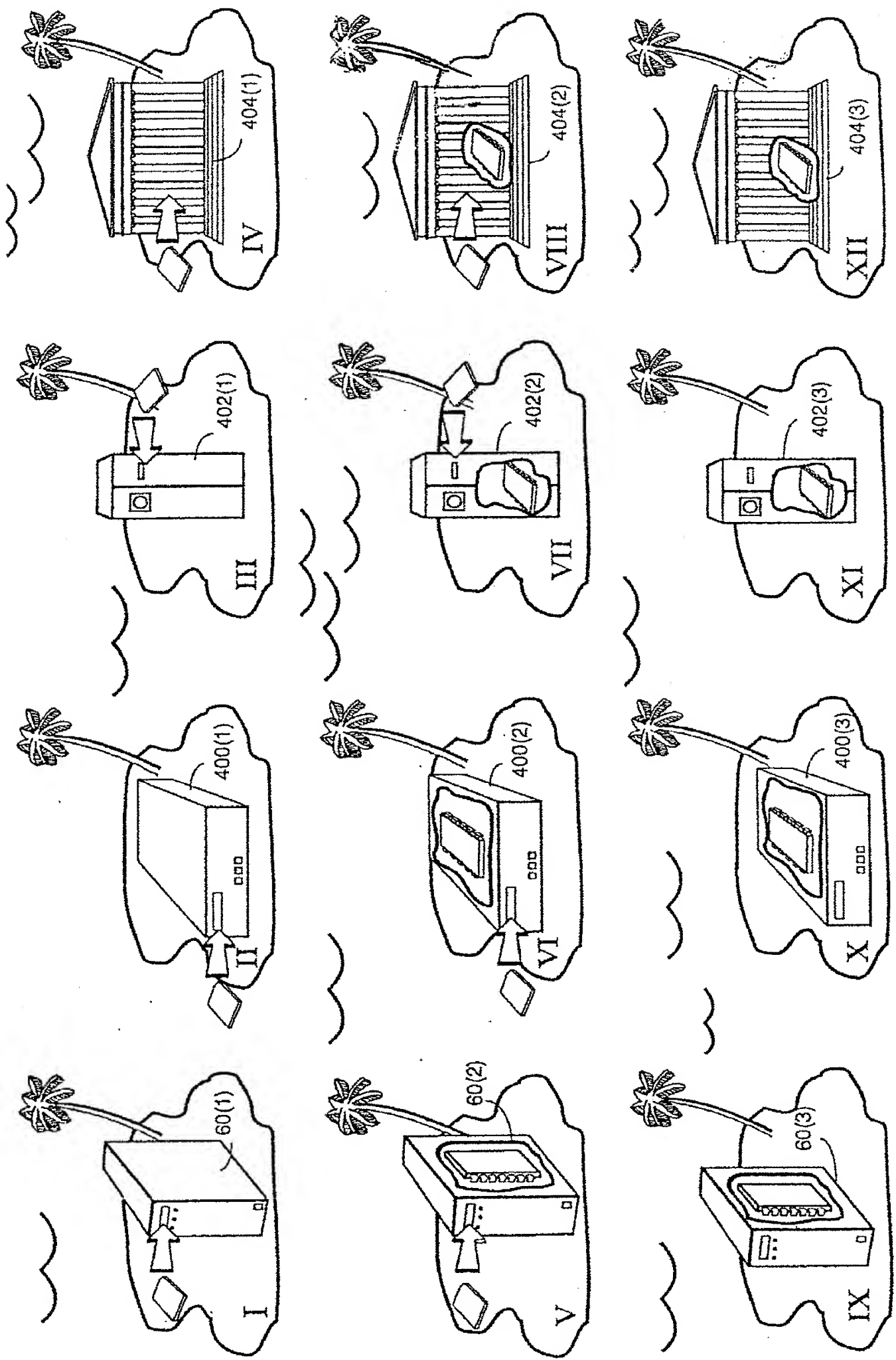
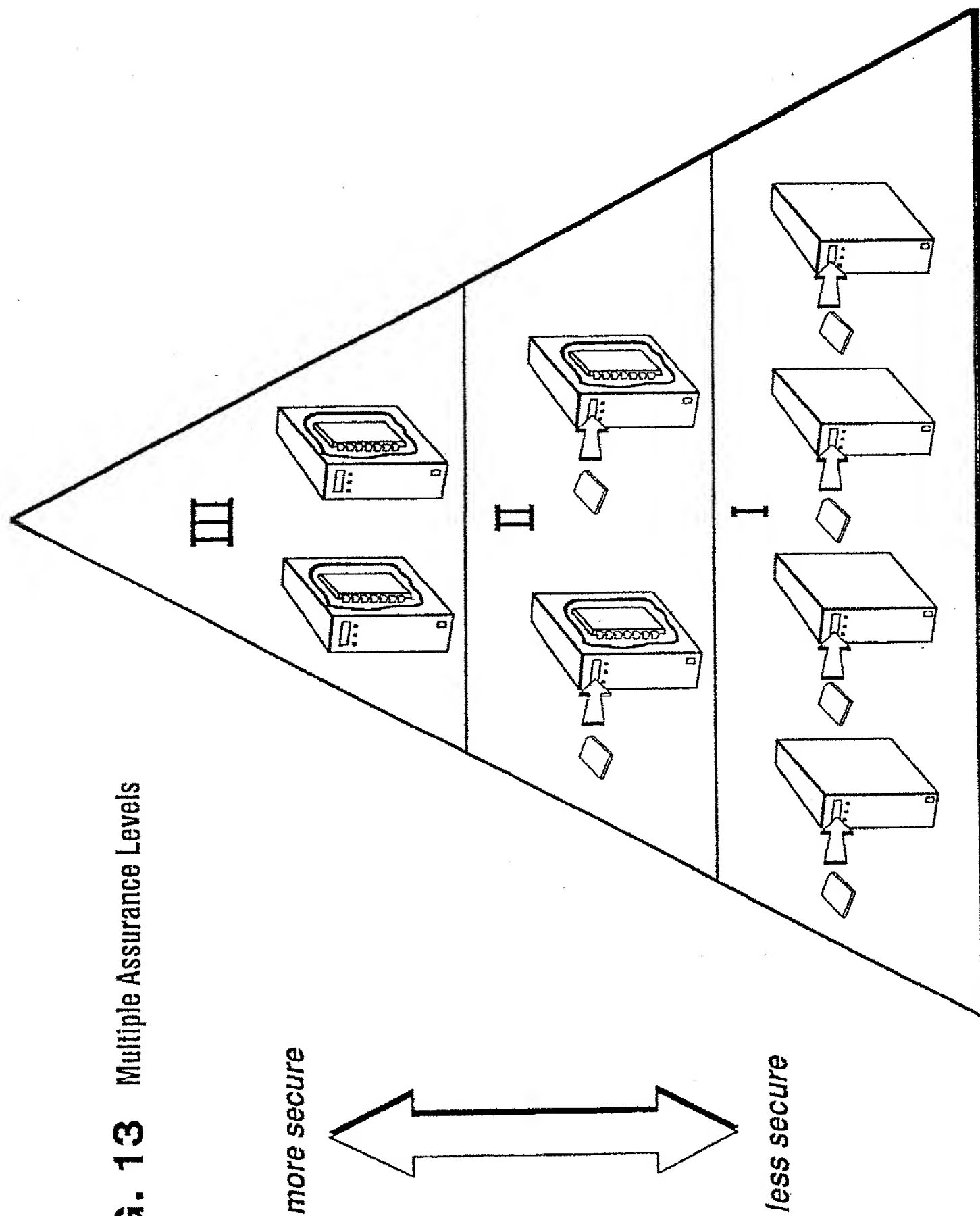


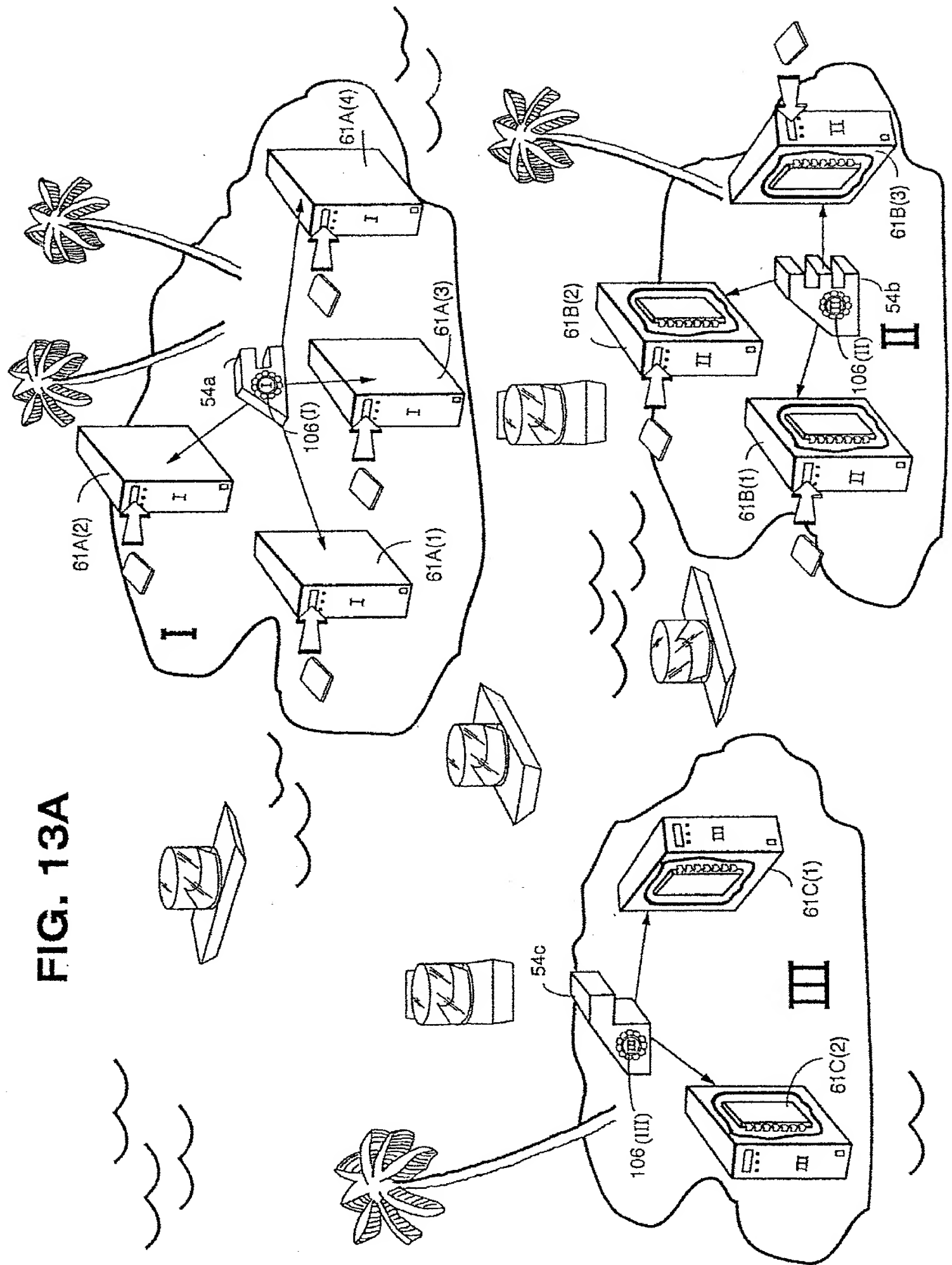
FIG. 12 Using Digital Signatures For Compartmentalizing Different Assurance Levels

# REPLACEMENT SHEET



**FIG. 13** Multiple Assurance Levels

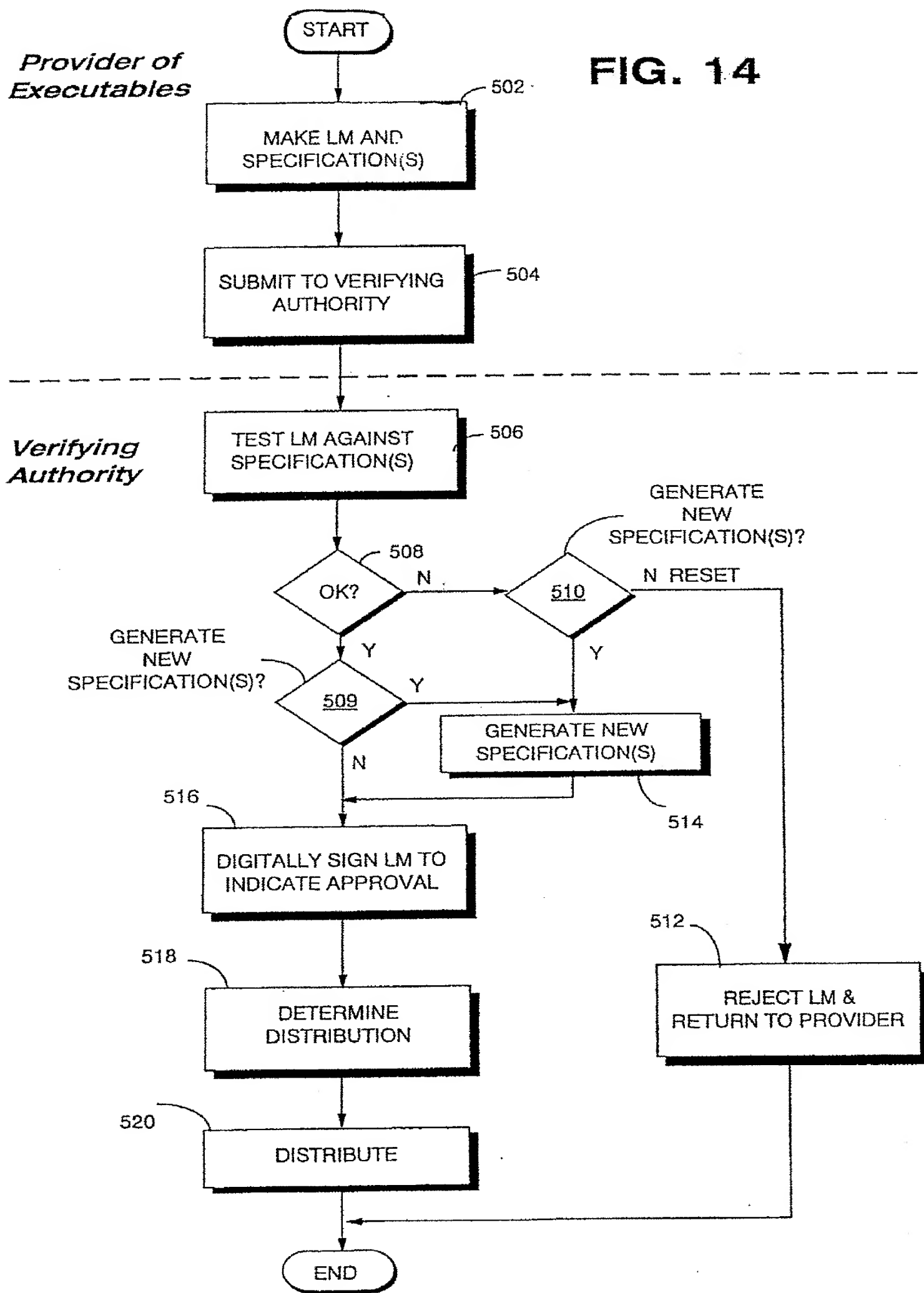
FIG. 13A

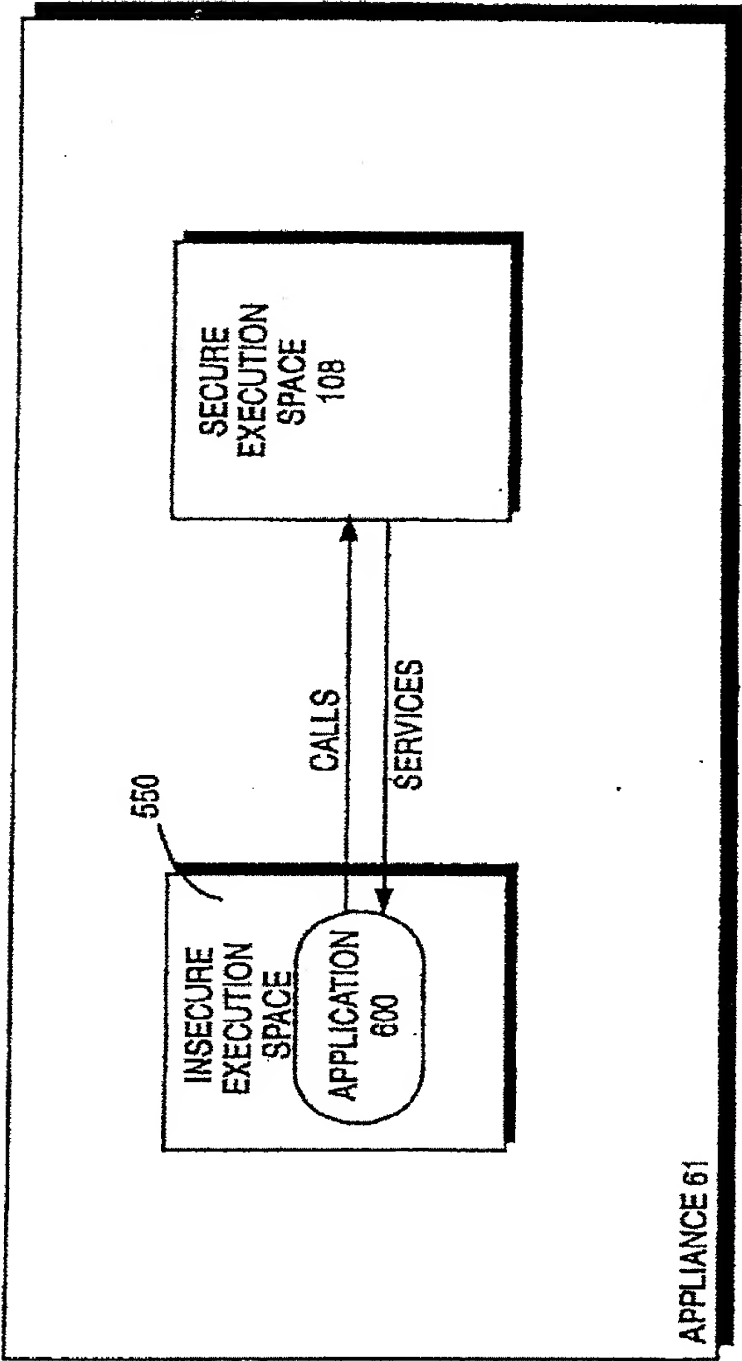


# REPLACEMENT SHEET

*Provider of Executables*

**FIG. 14**

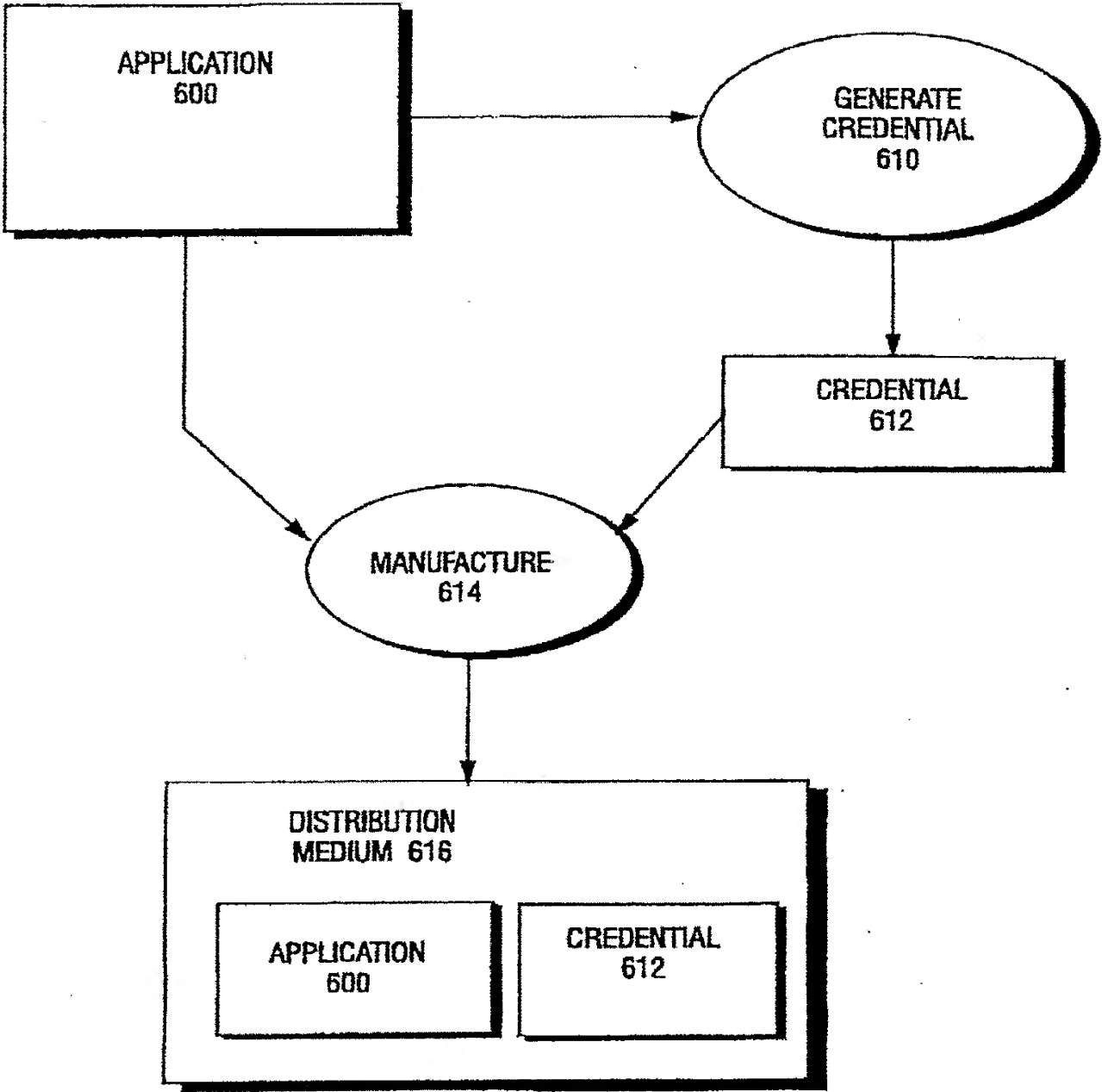




**FIG. 15** EXAMPLE APPLIANCE EXECUTING APPLICATION PROGRAM IN INSECURE EXECUTION SPACE

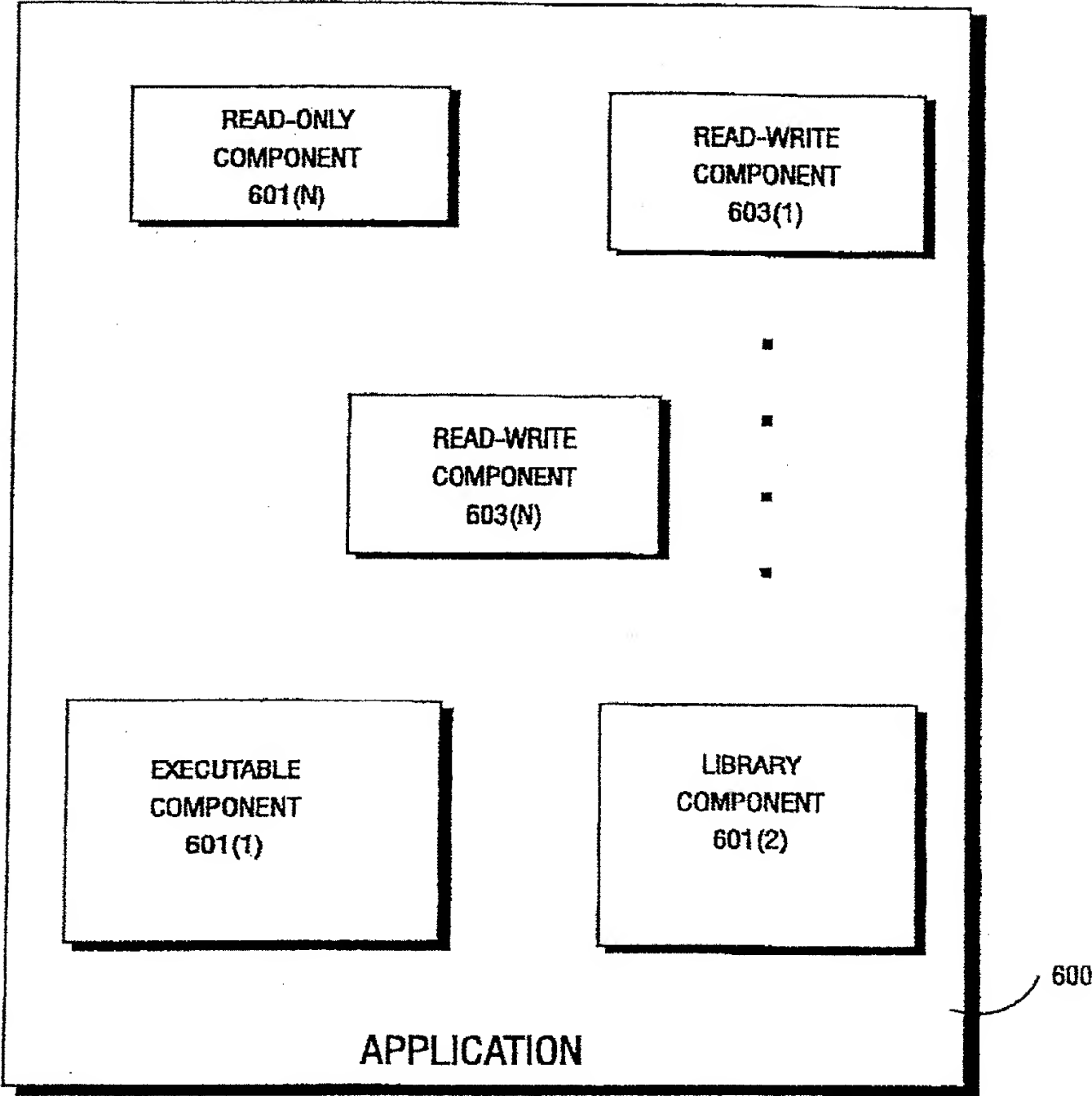


REPLACEMENT SHEET



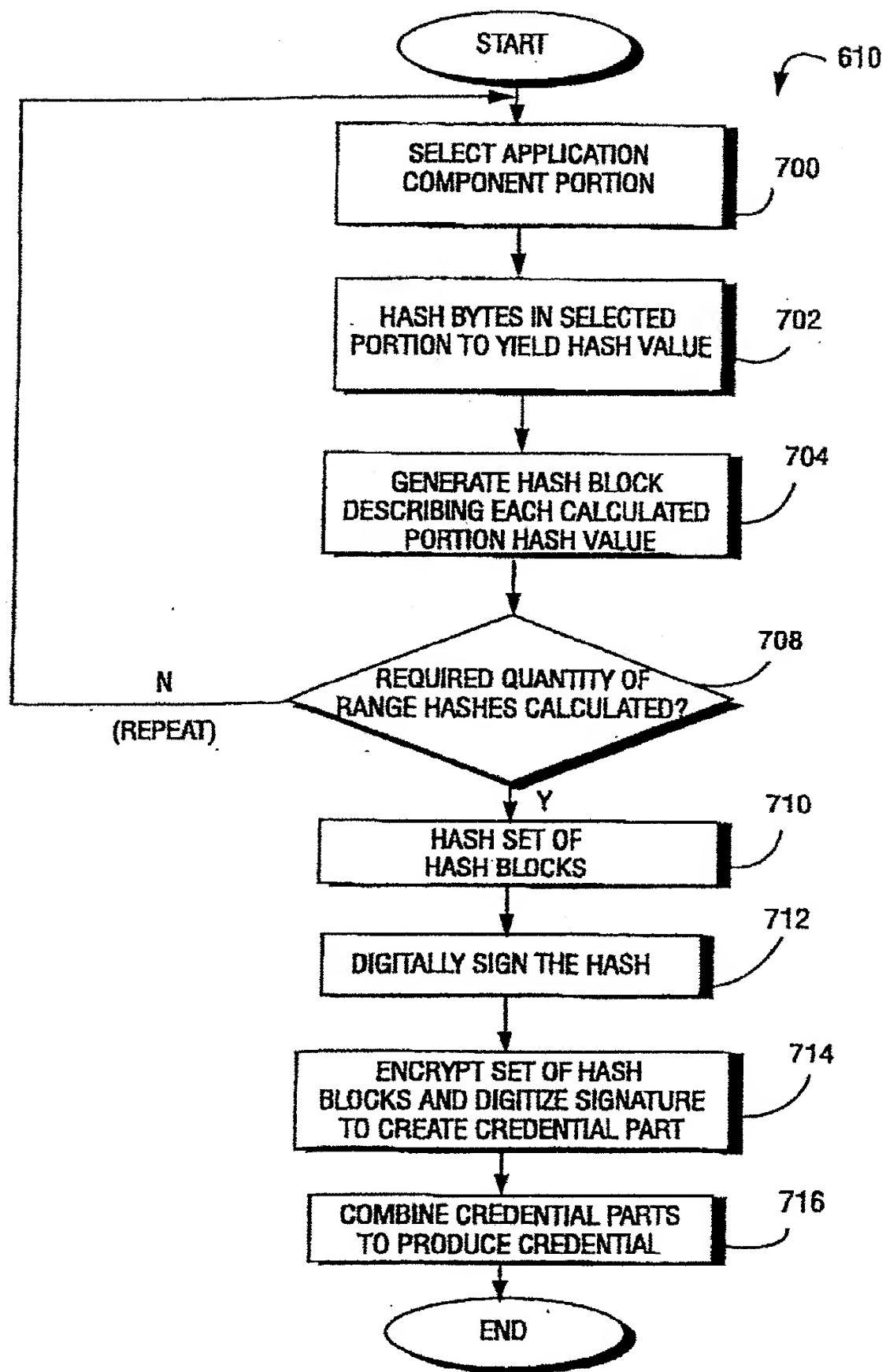
**FIG. 16** EXAMPLE APPLICATION CERTIFICATION PROCESS

REPLACEMENT SHEET



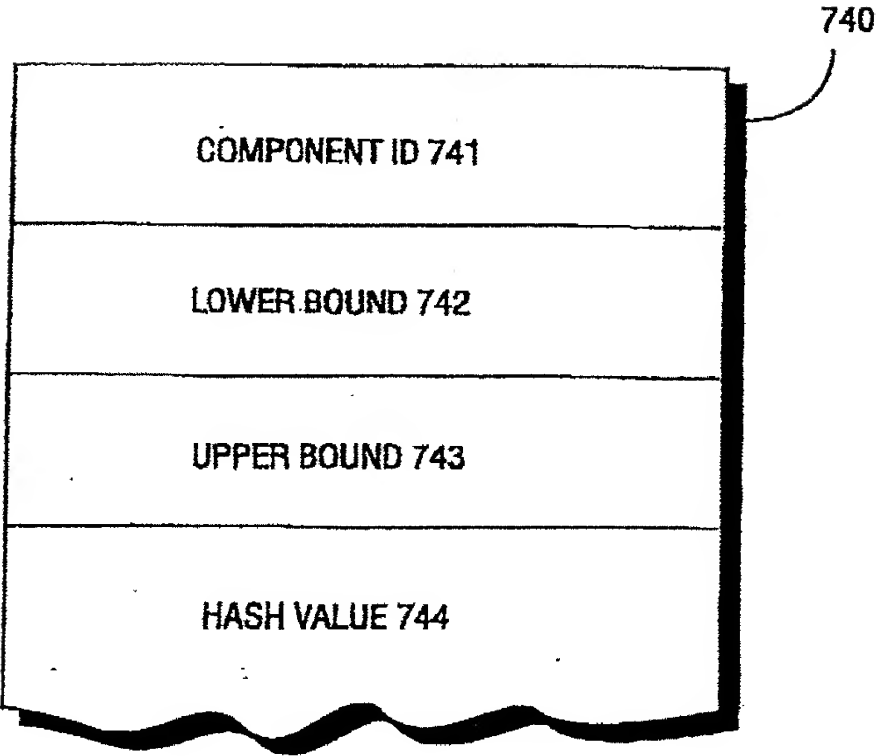
**FIG. 16A** EXAMPLE APPLICATION PROGRAM AND COMPONENTS

# REPLACEMENT SHEET



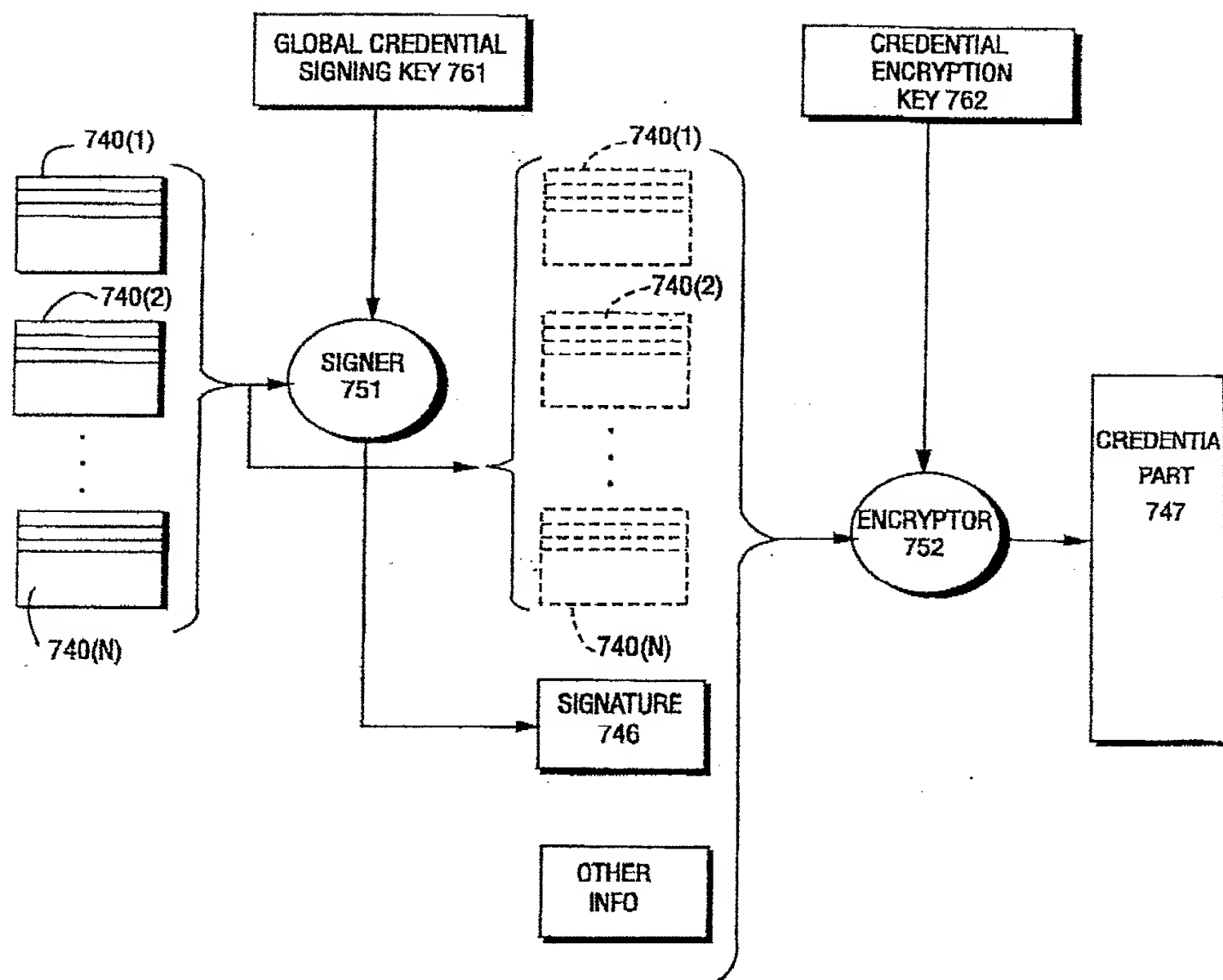
**FIG. 17** EXAMPLE CREDENTIAL CREATION PROCESS

REPLACEMENT SHEET



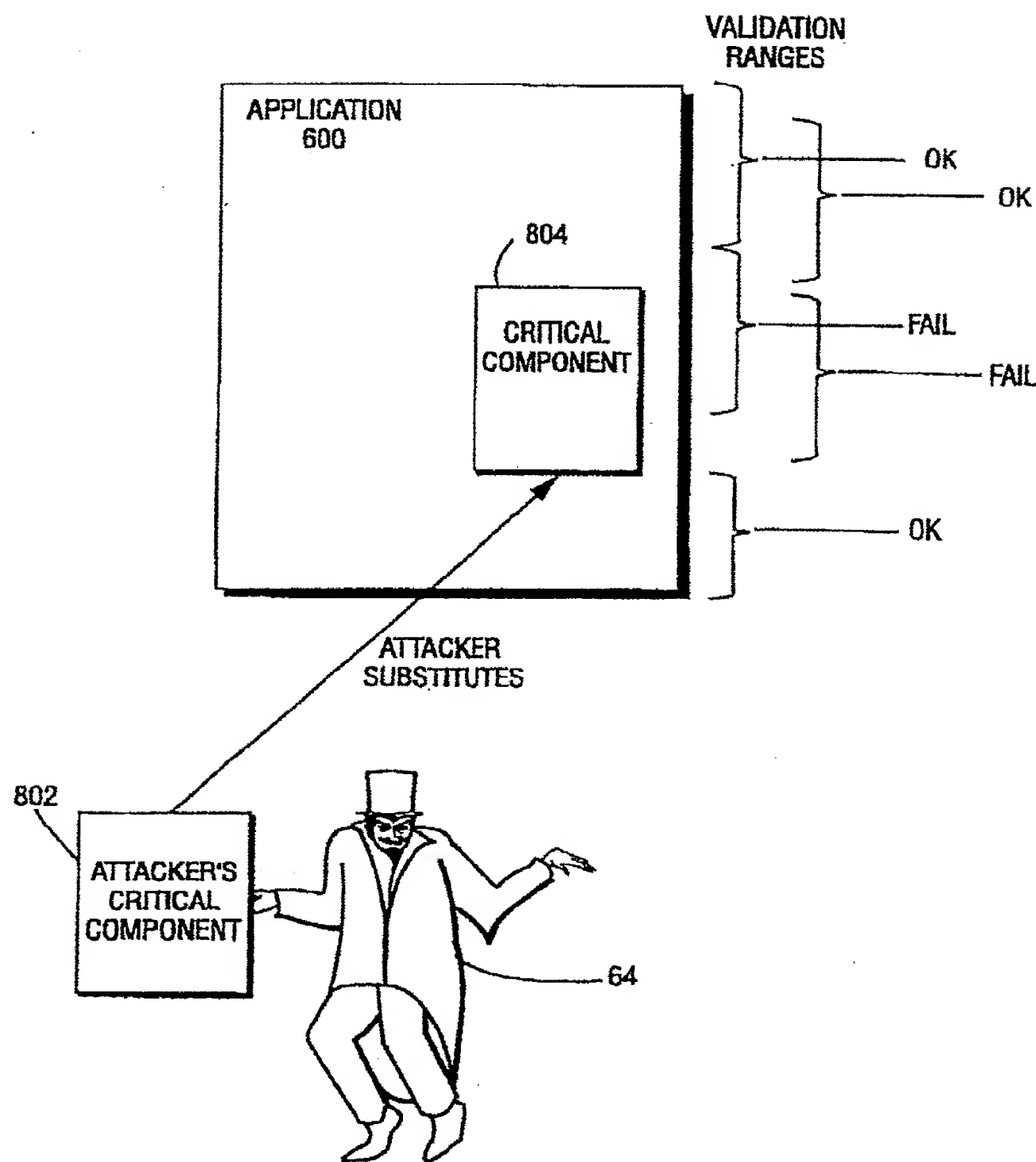
**FIG. 18** EXAMPLE HASH BLOCK

# REPLACEMENT SHEET



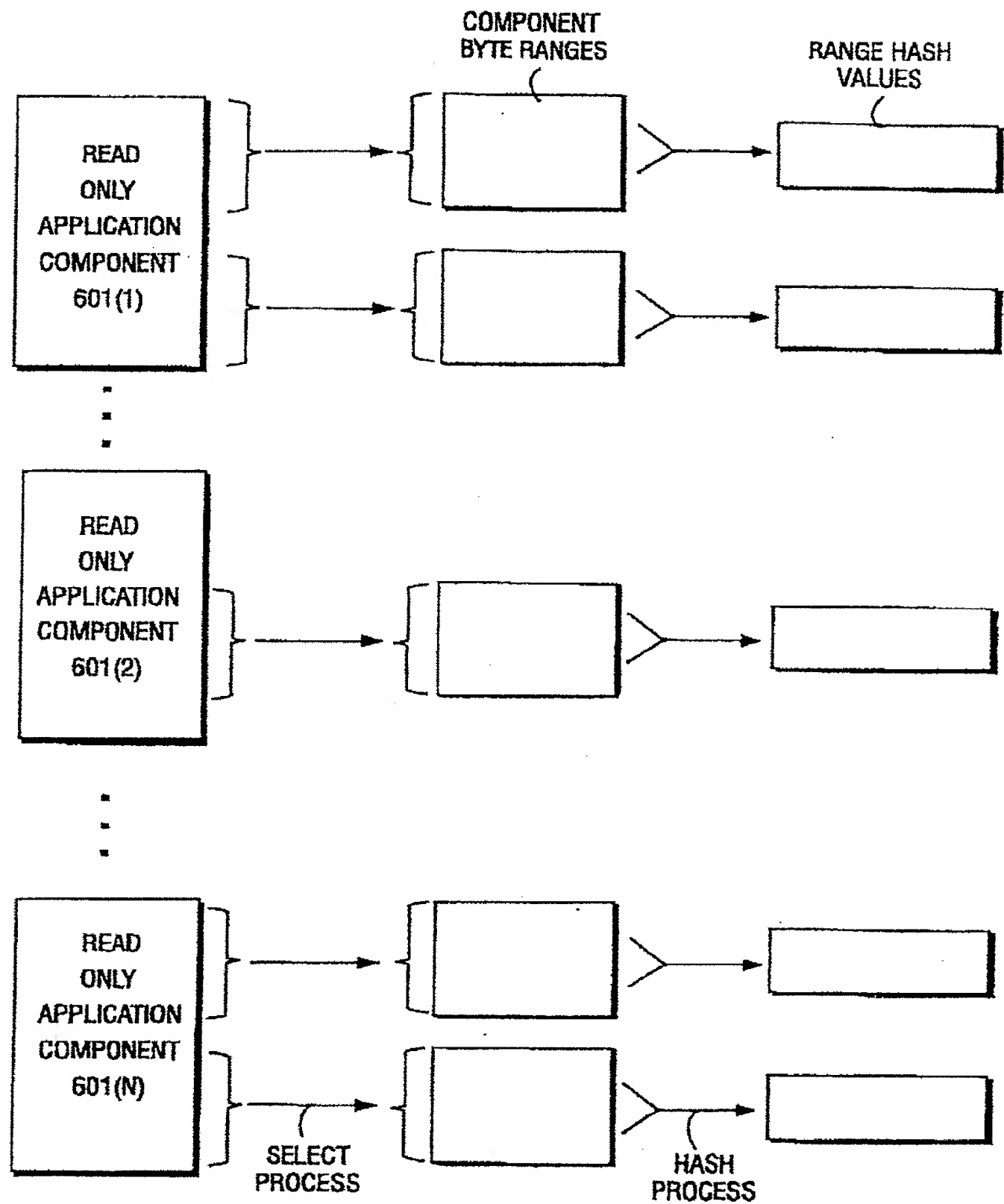
**FIG. 19** EXAMPLE CREDENTIAL CREATION

REPLACEMENT SHEET



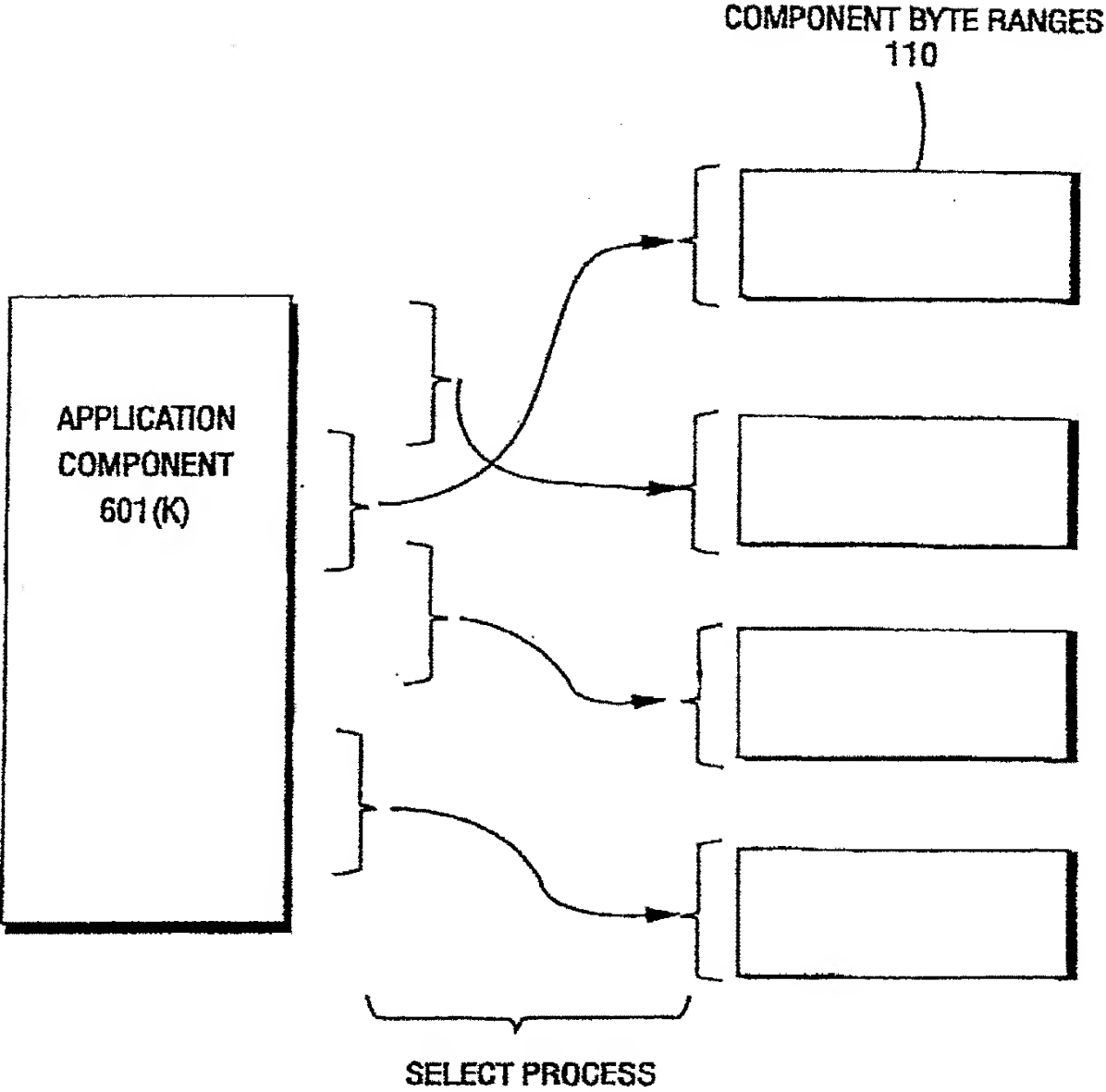
**FIG. 20** EXAMPLE ATTACK ON APPLICATION

# REPLACEMENT SHEET



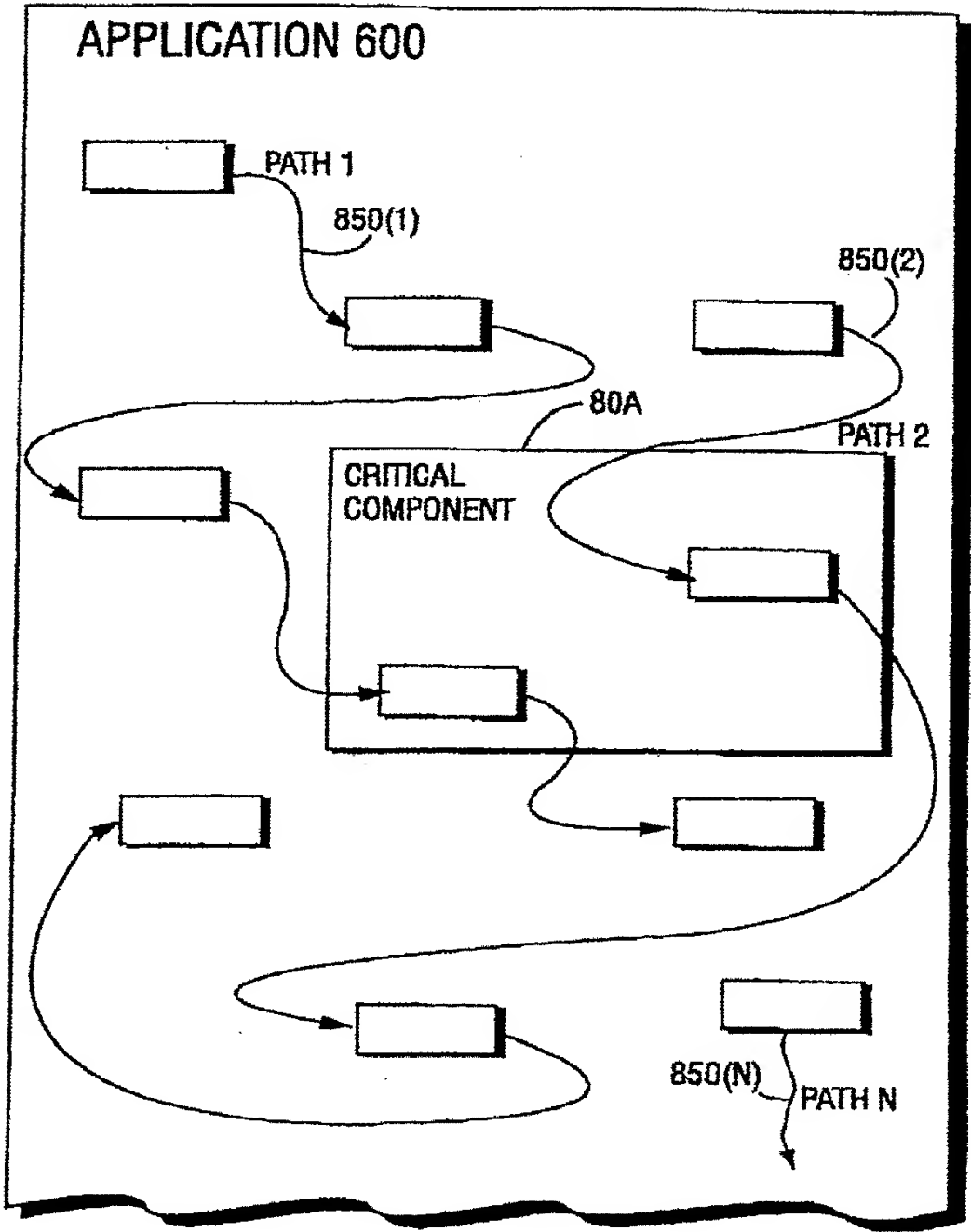
**FIG. 20A** EXAMPLE NON-OVERLAPPING HASH RANGES

REPLACEMENT SHEET

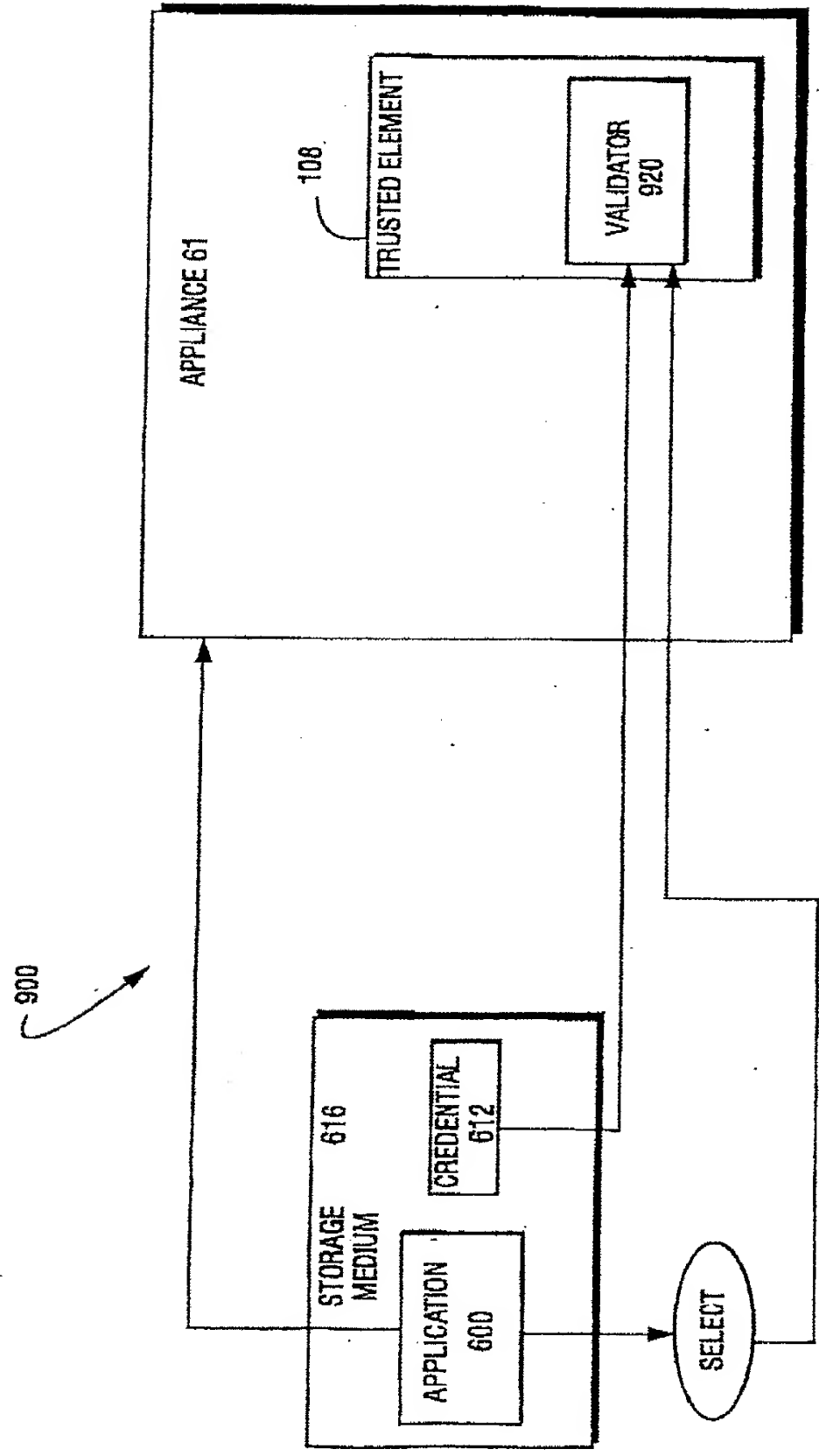


**FIG. 20B** EXAMPLE OF OVERLAPPING HASH RANGES





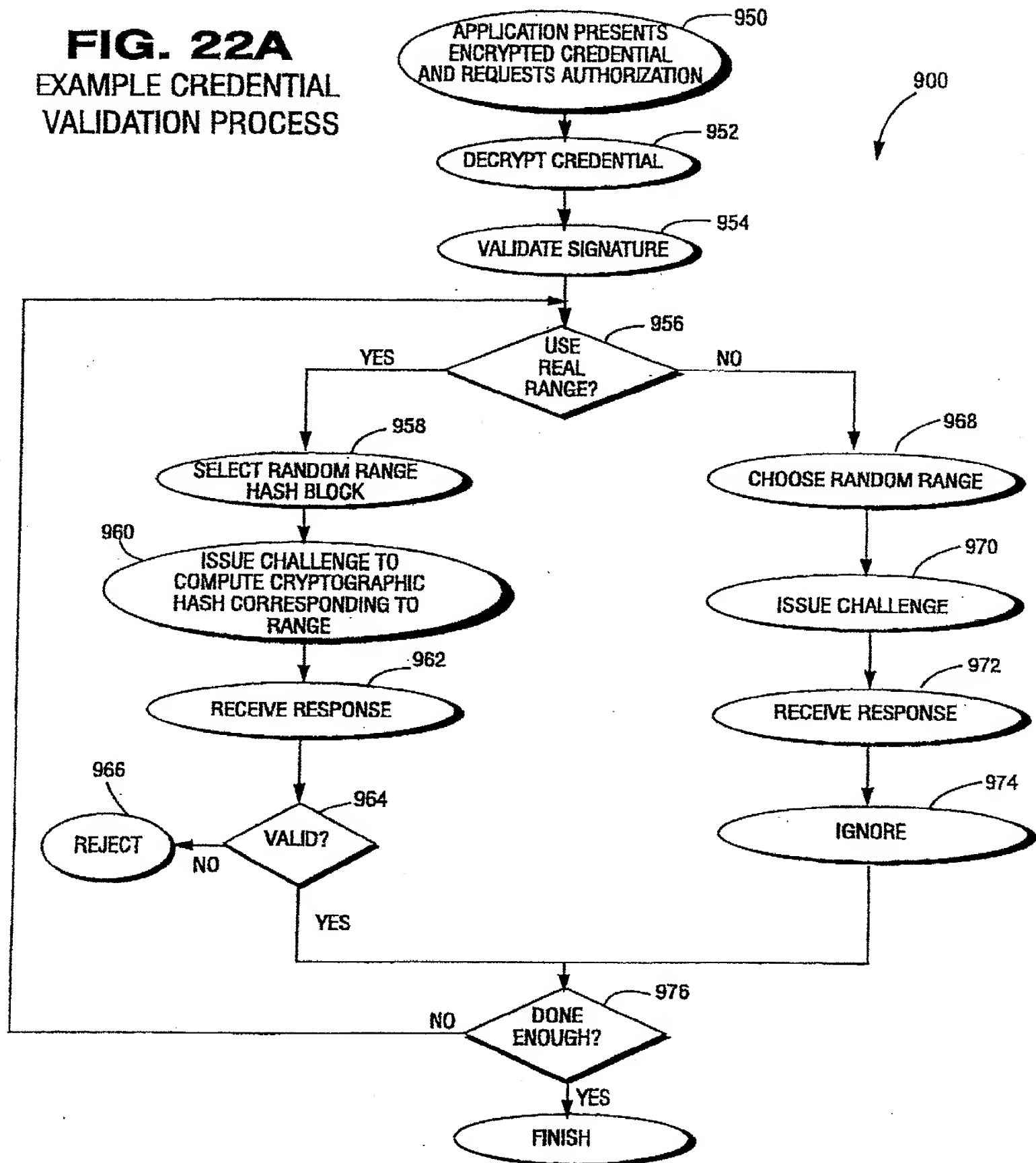
**FIG. 20C** PSEUDO-RANDOM VALIDATION PATHS IN APPLICATION



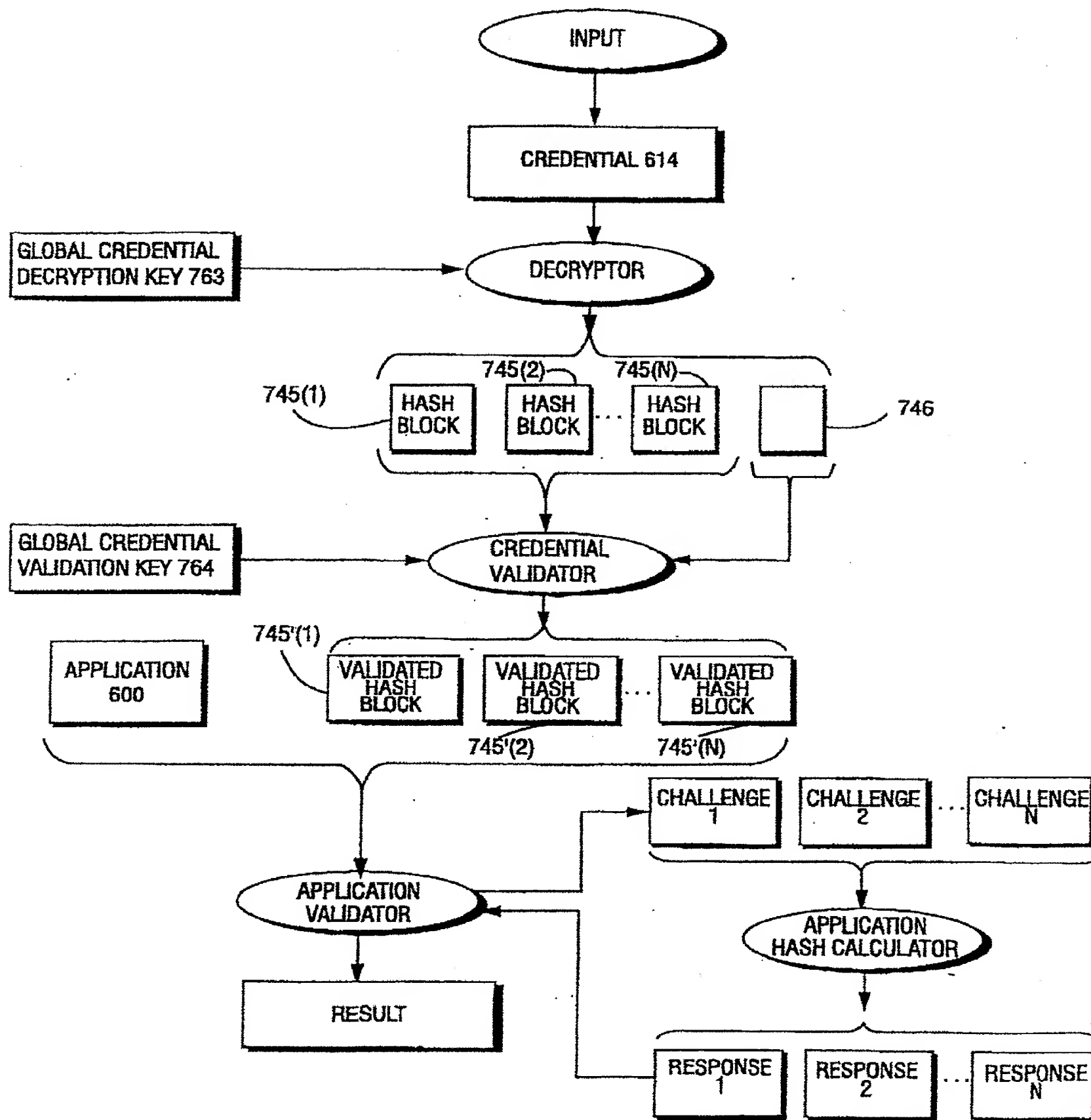
**FIG. 21** EXAMPLE CREDENTIAL VALIDATION PROCESS

# REPLACEMENT SHEET

**FIG. 22A**  
EXAMPLE CREDENTIAL  
VALIDATION PROCESS



# REPLACEMENT SHEET



**FIG. 22B** EXAMPLE CREDENTIAL VALIDATION